

REMARKS

Reconsideration of the present application, as amended, is respectfully requested. Claims 1-26 are pending in this application. Claims 1-26 are rejected. No claims have been added or cancelled. Claims 10, 13, and 24 have been amended without adding any new matter.

§102 Rejections

Claims 10-12 and 24-26 were rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 6,553,494 (hereinafter "Glass"). Applicants do not admit that Glass is prior art and reserve the right to swear behind the reference at a later date. Nonetheless, Applicants respectfully submit that claims 10-12 and 24-26 are not anticipated by Glass.

With regard to claims 10-12, the applicants claim "if the biometric identification matches a registered user on the BCS, receiving a certificate including a public key of the client certified by the BCS; and forwarding the certificate, including the public key of the client certified by the BCS, to the third party server, thereby identifying the client to the third party server."

Glass describes a detailed method of determining the identity of a signer of a document using a biometric sample from the system (Abstract, Column 6, lines 7-60). The process requires the original document, a unique token, biometric data, a secret encryption key, and an encrypted digital signature (Column 6, lines 7-18; Figure 2). Further, the process must decrypt the encrypted signature and compare it with an authentication hash value computed from two levels of hashing. However, the entire

process results in a document which is “accepted as having been signed by a signer” or biometric data used to “verify the identity of the individual using [the] biometric verification process” (Column 6, lines 18-60).

However, Glass fails to teach or suggest forwarding a certificate including a public encryption key to a third party server when a biometric certificate server (BCS) matches biometric data with a client certified by the BCS. In fact, Glass merely describes a two-party method of verifying an identity of a document signer based on an elaborate scheme, and not forwarding a public encryption key to a third party server requesting certification. This is shown in Figure 4 of Glass where the entire interaction occurs between personal computer (40) and central server (50). The personal computer (40) of Glass both requests and receives the digital signature from the server (50) (Figure 4; Column 8, line 57 to Column 9, line 15). Further, when a party desires to verify the digital signature, that party must directly send the central server (50) the document and receipt in order to receive verification from central server as to the authenticity of the digital signature (Figure 5; Column 9, lines 17-52). However, there is no “third party server” in Glass nor is a certification forwarded to the “third party server.”

Therefore, Glass fails to describe each element claimed by the Applicants in claim 10. Accordingly, the Applicants respectfully submit that the invention as claimed in claims 10-12 is not anticipated by Glass under 35 U.S.C. § 102(e) for at least the reasons discussed above.

With regard to claims 24-26, the applicants claim:

a crypto-server having a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection;
an authentication engine to authenticate a user of the client based on biometric data of the user;

a cryptographic engine to use the user's private key, as a virtual smart card, to perform the requested cryptographic function after the user has been authenticated by the authentication engine; and the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.

The Applicants respectfully submit that Glass fails to describe each element as claimed by the Applicants in claims 24-26.

As discussed above, Glass describes an elaborate process wherein biometric data can be coupled with a document to provide an identify verification tool or a document integrity verification tool (Abstract; Column 4, lines 26-39; Column 6, lines 7-60). Further, the process utilizes an encryption key in the verification process (Figures 1-3, element 24). The key described by Glass in creating the verifiable digital signature, however, is associated with a camera used to obtain biometric data (Column 4, lines 26-39).

With regard to claims 24-26, the Applicants claim “an authentication engine to authenticate a user of the client based on biometric data of the user; [and] a cryptographic engine to use the user's private key, as a virtual smart card, to perform the requested cryptographic function after the user has been authenticated by the authentication engine” (Emphasis Added). That is, the crypto-server retains, controls, and then uses a user's private encryption key after the user has been authenticated by the server. However, the camera of Glass used to create the digital signature and the server of Glass used to verify the digital signature explicitly use the camera's encryption key and not a user's key (Glass, Column 4, lines 46-50).

For the sake of argument, even if the camera is seen as a user such that the camera/user's encryption key is used to create the digital signature, the camera remains

in control of the encryption key. That is, the camera/user controls and applies its own encryption key in the digital signature process. The camera must also provide its key for an authentication process. Thus, a server does not retain, control, and use an encryption key of a user, as claimed by the Applicants.

Therefore, Glass fails to describe a cryptographic engine that uses a user's private key to perform a requested cryptographic function, as claimed by the Applicants. Accordingly, the Applicants respectfully submit that the invention as claimed in claims 24-26 is not anticipated by Glass under 35 U.S.C. § 102(e) for at least the reasons discussed above.

§ 103 Rejections

Claims 1-4, 6-9, 22, and 23 were rejected under 35 U.S.C. § 103(a) as being obvious over Glass in view of U.S. Patent No. 5,535,276 (hereinafter "Ganesan"). The Applicants respectfully disagree because the combination of Glass and Ganesan fail to teach or suggest each and every element of the invention as claimed in claim 1-4, 6-9, 22, and 23.

As discussed above, Glass describes an elaborate method of creating a digital signature that is composed of biometric data, a private encryption key, and a unique token (Abstract; Column 6, lines 7-60). This information can further be transmitted to a server for storage in the form of a certificate triggering the server to generate and return a receipt associated with the certificate (Column 9, lines 9-15). Then at some later time, biometric data can be provided to the server along with a document and the document's purported receipt for verification. However, as admitted by the examiner Glass only

provides a verification service and fails to describe: “generating a disposable public key/private key pair if the user is authenticated based on the biometric data,” as claimed in claim 1.

Ganesan describes a system of providing a secure communication connection (Abstract; Column 8, lines 9-43). The connection is secured when a first user generates a temporary key pair, on the user’s computer, to encrypt a message and exchanges the pair and message with a server (Column 8, lines 20-25). This method allows another user to then further encrypt a message when that user generates their own temporary key pair so that both users can authenticate each other through the server. Thus, each temporary key pair is generated by the communication initiator (Column 8, lines 40-44; Column 9, lines 17-54). However, Ganesan does not teach generating the encryption keys on a server separate from the user if the user is authenticated based on biometric data.

The applicants, claim “the BCS generating a disposable public key/private key pair if the user is authenticated based on the biometric data” in independent claim 1. That is, a server generates a disposable public key/private key pair after user authentication, such that the user is not required to create the disposable key pair. The Examiner admitted that Glass fails to teach generating a key pair (Office Action, page 5, section 7). Furthermore, as discussed above, temporary key pairs are generated in Ganesan by a communication initiator, and not a server. Therefore, neither Glass nor Ganesan, alone or in combination, teach or suggest a biometric certification server “generating a disposable public key/private key pair if the user is authenticated based on the biometric data.” Thus, claim 1 is not rendered obvious under 35 U.S.C. § 103

over Glass in view of Ganesan. Furthermore, dependent claims 2-4 and 6-9 which depend from claim 1 are also not rendered obvious under 35 U.S.C. § 103.

With respect to independent claim 22, the applicants claim “the remote crypto-server to generate a disposable public key/private key pair and perform the requested cryptographic function when the user is successfully authenticated using the biometric data.” Similar to the discussion above, neither Glass nor Ganesan describe or suggest a remote crypto-server to generate a public key/private key pair when a user is authenticated using biometric data. Therefore, claim 22 is not rendered obvious under 35 U.S.C. § 103 over Glass in view of Ganesan.

With respect to independent claim 23, the applicants claim a crypto server that generates a disposable public key/private key pair and performs a cryptographic function, where the crypto server further authenticates a user based on biometric data. For reasons similar to the discussion above, neither Glass nor Ganesan describe or suggest the crypto server to generate a disposable public key/private key pair as claimed in claim 23. Therefore, claim 23 is also not rendered obvious under 35 U.S.C. § 103 over Glass in view of Ganesan.

Claim 5 was rejected under 35 U.S.C. § 103 as being unpatentable over Glass in view of Ganesan, and further in view of U.S. Patent No. 6,553,494 of Brickell et al. (hereinafter “Brickell”). As noted above with respect to independent claim 1, from which claim 5 depends, neither Glass nor Ganesan describe or suggest “the BCS generating a disposable public key/private key pair if the user is authenticated based on the biometric data.” Brickell merely discusses a digital signature system (Abstract; Column 3, line 45-65; Column). The digital signature system may limit access to the system by requiring

a trusted token, where the token includes a personal identification numbers, a PC card, or biometric data, for accessing the system, (Column 16, lines 28-65). Therefore, Brickell does not overcome the shortcomings of Glass in view of Ganesan. Thus, the combination of Glass, Ganesan and Brickell fails to teach or suggest “the BCS generating a disposable public key/private key pair if the user is authenticated based on the biometric data,” as claimed in claim 1. Thus, neither Glass, Ganesan, nor Brickell describe or suggest “the BCS generating a disposable public key/private key pair if the user is authenticated based on the biometric data” as claimed in claim 1. Since claim 5 depends from independent claim 1, claim 5 is also not taught or suggested by the combination of Glass, Ganesan, and Brickell. Thus, the Applicants submit that claim 5 is not rendered obvious under 35 U.S.C. § 103 over Glass in view of Ganesan and further in view of Brickell.

Claims 13-21 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Glass in view of U.S. Patent No. 6,587,946 of Jakobsson (hereinafter “Jakobsson”). The Applicants respectfully disagree because the combination of Glass and Jakobsson fail to teach or suggest each and every element of the invention as claimed in claims 13-21.

Claim 13, as amended, claims:

a crypto-server having a crypto-proxy interface for receiving a request for a cryptographic function from a client on a secure connection;

an authentication engine for authenticating the user based on biometric data received through the crypto-proxy interface of the crypto server;

a cryptographic engine for performing the cryptographic functions after the authentication engine has authenticated the user based on the biometric data; and

the crypto-proxy interface for returning data to the client, after the cryptographic functions are performed.

The Applicants respectfully submit that claim 13, as amended, is not rendered obvious by Glass in view of Jakobsson.

As discussed above, Glass describes an elaborate method of creating a document signature that consists of a person's biometric data, a private encryption key, and a unique token (Abstract; Column 6, lines 7-60). The signature can then be used as a way to authenticate a person as the signer of the document, where the signature consists of the person's biometric data, a known encryption key, and a known token. Thus, Glass merely provides a system for verifying a digital signature where the digital signature has been encrypted.

Jakobsson describes a system for providing an encrypted message to a second recipient when the primary recipient is unavailable (Column 3, lines 9-15; Column 5, lines 1-47). In the system, portions of the primary recipient's private encryption key are shared among a quorum of proxy servers (Column 3, lines 37-41; Column 7, lines 25-28). Each of the proxy servers modifies the message so that it can be delivered to a secondary recipient such that the secondary recipient can decipher the message (Abstract). However, Jakobsson fails to discuss the use of biometric data in the messaging system.

The Applicants, however, claim a crypto-server having a crypto-proxy interface that receives requests for cryptographic functions, receives biometric data, and returns data to a client after the cryptographic function has been performed. Further, the cryptographic function is performed after a user has been authenticated by an

authentication engine of the crypto-server. The Examiner admitted that Glass fails to teach or suggest a crypto-server having a crypto-proxy interface for receiving requests for cryptographic functions (Office Action, page 9, section 9). Since Glass fails to teach any form crypto-server, Glass also fails to teach or suggest a crypto-server for further receiving biometric data of a user. Furthermore, as discussed above, the messaging system described in Jakobsson fails to teach or suggest the use of biometric data in messaging process or the messaging proxy servers. Thus, Jakobsson also fails to teach or suggest a crypto-server for receiving requests, receiving biometric data, and returning data after the requested cryptographic function is performed and the user is authenticated. Therefore, neither Glass nor Jakobsson, teaches or suggests a crypto-server having a crypto-proxy interface that receives requests for cryptographic functions, receives biometric data, and returns data to a client after the cryptographic function has been performed and the biometric data of the user has been authenticated.

Therefore, since neither Glass nor Jakobsson teach or suggest each and every element as claimed in claim 13, and claim 13 is not rendered obvious under 35 U.S.C. § 103 by Glass in view of Jakobsson. Further, since claims 14-21 depend from claim 13, claims 14-21 are also not rendered obvious under 35 U.S.C. § 103 by Glass in view of Jakobsson.

Conclusion

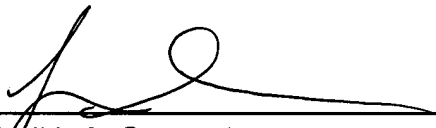
Applicant respectfully submits that in view of the amendments and discussion set forth herein, the applicable rejections have been overcome. Accordingly, the present and amended claims should be found to be in condition for allowance.

If a telephone interview would expedite the prosecution of this application, the Examiner is invited to contact Judith Szepesi at (408) 720-8300.

If there are any additional charges/credits, please charge/credit our deposit account no. 02-2666.

Respectfully submitted,
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Dated: 12/19/06



Judith A. Szepesi
Reg. No. 39,393

Customer No. 08791
12400 Wilshire Blvd.
Seventh Floor
Los Angeles, CA 90025
(408) 720-8300